Remarks:

Applicants have read and considered the Office Action dated May 16, 2006 and Notice of Non-Compliant Amendment dated October 25, 2006. Claims 20-26 have been amended. Claims 19 and 28 have been cancelled without prejudice or disclaimer. New claims 29-41 have been added. Claims 20-26 and 29-41 are currently pending.

The specification was objected to as it lacks any mention of "the body of integers modulo n" that is recited in the claims. The claims have been amended to recite "the ring of integers modulo n." Applicants assert that there is support for this term in the specification and Applicants assert that the objection to the specification is overcome.

The claims were objected to for a number of informalities. Claims 20-23 and 25-26 use "x" to represent multiplication. The Action asserts that this is inconsistent with the independent claims and the specification. The claims have been amended so that a proper multiplication "•" is used. Claims 24, 25 and 26 recite "the" process. Claims 24 and 25 have been rewritten in independent form and claim 26 refers to the computer implemented process. Claim 28 has now been cancelled. Applicants assert that the claims overcome the objection.

Claims 19-26 and 28 were rejected under 35 U.S.C. § 112 first paragraph as failing to comply with the written description requirement. The Action asserts that "the body of integers modulo n" lacks support. The Action notes that there is support for "the ring of integers modulo n". The claims have been amended and recite "the ring of integers modulo n" and Applicants assert that there is proper support.

Claims 19-26 and 28 were rejected under 35 U.S.C. § 112 as being indefinite. The Action asserts that the use of parenthesis renders the claims unclear. The parenthesis have been deleted from the objected to portions. Applicants assert that the indefiniteness rejection has been overcome.

Claims 19, 25 and 28 were rejected under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter. Claims 19 and 28 have been cancelled. Claim 25 has been amended to recite additional steps and is believed to meet the statutory requirements of 35 U.S.C. § 101.

Claims 19-26 and 28 were provisionally rejected on the grounds of non-statutory obviousness-type double patenting as being unpatentable over claims 19-28 of co-pending Application No. 10/089,662. Applicants assert that the claims of the two applications are patentably distinct from each other. The two systems are trying to solve the equation $G_i=Q^v \bmod n$. The analysis of the systems described in the two applications is radically different. The present application recites specific mathematical steps with equations and conditions recited in the claims. The recited steps, equations conditions are nontrivial and the claims are patentably distinct over 10/089,662, which does not recite particular mathematical conditions in the claims. Applicants assert that the combination of the method steps reciting the particular non-obvious equations is patentably distinct from and patentably distinguishes over 10/089,662. Therefore, the obviousness-type double patenting rejection is improper. Moreover, Applicants assert that the ***present invention has priority*** and that both applications should not be restricted with a Terminal Disclaimer. Applicants further assert that the remaining issues have been resolved and that the only remaining rejection is a provisional obviousness-type double patenting rejection, the rejection should be withdrawn and this application should be allowed to issue. See MPEP § 804. Applicants request that the double patenting rejection be withdrawn.

Claims 19-26 and 28 were provisionally rejected on the ground of non-statutory obviousness-type double patenting as being unpatentable over claims 1-20 of co-pending Application No. 09/889,958. Applicants assert that Application No. 09/889,958 has been abandoned and the rejection is moot.

Finally, claims 19-26 and 28 were provisionally rejected on the grounds of non-statutory obviousness-type double patenting as being unpatentable over claims 13-24 of co-pending

Application No. 09/869,966. Applicants assert that the claims are patentably distinct. Applicants assert that 09/869,966 is directed to precisely describing how one "obtains" adequate values for keys and describes different steps of calculation for allowing one to obtain such keys, but is directed only to how one obtains the values. The claims of the present application recite ***both obtaining and using*** a set of cryptographic keys obeying certain non-obvious mathematical constraints. Applicants assert that the claims of the present application are directed to patentably distinct subject matter and the claims patentably distinguish over the cited application. Applicants assert that the provisional double patenting rejection should be withdrawn for these reasons as well as those discussed above.

New claims 29-31 have been added and depend from claim 21. Applicants assert that claims 29-31 are allowable for at least the reasons discussed above with respect to claim 21.

New independent claim 32 recites a computer readable medium storing instructions which cause a processor to execute a method. The method includes obtaining a set of one or more private values, receiving a commitment from a demonstrator, choosing challenges randomly, sending the challenges to the demonstrator, receiving a response from the demonstrator and determining that the demonstrator is authentic if the response has a particular value. Moreover, Applicants assert that this is neither shown nor suggested by the prior art. Applicants assert that claim 32 is allowable for reasons similar to those in claim 21.

New claim 33 also recites a method carried out by the processor. Applicants assert that claim 33 recites a storage medium performing a method that is neither shown nor suggested by the prior and is also allowable for the reasons similar to those recited for claim 21.

New claim 34 recites a computer readable medium storing instructions that cause a processor to execute a method including obtaining a set of one or more private values, receiving a token from a demonstrator, choosing challenges randomly, sending the challenges to the demonstrator, receiving a response from the demonstrator, and determining that the message is

authentic if the response has a particular value. Applicants assert that the recited storage medium performing such a method is neither shown nor suggested by the prior art or any combination thereof. Applicants assert that new claim 34 is allowable for reasons similar to the reasons that claim 22 is allowable. Similarly, new claim 35 is believed to recite a similar method with a computer readable medium and Applicants assert that claim 35 is allowable for similar reasons. In addition, claims 36-39 depending from claims 32-35 respectively, are also allowable for these reasons as well as others associated with advantageous use of challenges.

New independent claim 40 recites a computer readable medium storing instructions that cause a processor to execute a method including obtaining a set of one or more private values, recording a message to be signed, choosing integers randomly, computing commitments with a particular value, computing a token having a particular value, identifying bits of the token and computing responses. Applicants assert that a medium executing such a method is neither shown nor suggested by the prior art or any combination thereof. Applicants assert that claim 40 is therefore allowable over the prior art. Applicants assert that claim 40 is allowable for reasons similar to the reasons that claim 25 is believed to be allowable. In addition, claim 41 provides further advantages regarding collecting the token and determining the message that is neither shown nor suggested by the prior art. Applicants assert that claims 40 and 41 are therefore allowable.

Applicants assert that the claims are in condition for allowance. A speedy and favorable action on the merits is hereby solicited. If the Examiner feels that a telephone interview may be helpful in this matter, please contact Applicants' Representative at (612) 336-4728.

Respectfully submitted,

MERCHANT & GOULD P.C.

Dated: 11/16/06

By: _____
Gregory A. Sebald
Reg. No. 33,280
GAS/krn